**National Association of Independent Insurers ("NAII")**

**Gramm-Leach Bliley Act ("GLB") Privacy Rules**

**16 CFR Part 313 - Comments to the**

**FEDERAL TRADE COMMISSION**

**12 CFR Part 332 - Comments to the**

**FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)**

**12 CFR Part 216 - Comments to the**

**FEDERAL RESERVE SYSTEM (FRS)**

**Board of Governors of the Federal Reserve System**

**12 CFR Part 573 - Comments to the**

**DEPARTMENT OF THE TREASURY**

**Office of Thrift Supervision**

**12 CFR Part 40 - Comments to the**

**DEPARTMENT OF THE TREASURY**

**Office of the Comptroller of the Currency**

**March 31, 2000**

**Overview**

The National Association of Independent Insurers (NAII) is a trade association of 650 property and casualty insurers writing all lines of business in all states. For the most recent year data were available, NAII members wrote over $92.48 billion in premium. NAII respectfully submits these comments to the proposed rules of the federal regulators.

While it is believed that these comments will generally track with the notice of proposed rulemaking of each of the regulators, the Notice of Proposed Rulemaking of the Federal Trade Commission (FTC) was used as a template for making these comments.

**General Comments**

NAII appreciates that underlying the GLB Act is the concept of functional regulation. While the GLB Act leaves the regulation of the business of insurance to the states, NAII also believes that to a large extent privacy rules adopted by the federal regulators will be generally adopted at the state level as to the business of insurance. On this basis, it is appropriate for NAII to comment to the federal rules. In addition, it is likely that under financial services modernization, banks, insurers, and securities firms will be dealing extensively with each other, whether on an affiliated basis or not. For the ease of transaction of business, privacy rules at the federal level must address the needs of the insurance segment of the financial services industry.

These comments are directed to the federal regulators as a unit to stress the need for uniformity across federal regulatory lines in regard to privacy rules. One purpose of the

GLB Act is to permit affiliations among financial entities. Streamlining of financial services, if you will. Now that GLB is law, it is imperative that the privacy rules for each of the federal regulators be uniform to minimize unnecessary cost of business which would exist should one or more of the federal regulators "break ranks" to have a unique set of privacy requirements. In effect, NAII urges the federal regulators to streamline the privacy rules. NAII urges the federal regulators to find uniformity while balancing the need to protect consumer privacy with the need for making personal information available to inform the public of product availability. This theme underlies the comments contained herein.

Certain issues relating to the privacy rules are appropriate for comment outside those specifically requested by the FTC notice. The first of these is the concept of "opt-out". The goal of the federal regulators should be to strike a balance between protection of personal information and the valid use of that same information. Opt-out preserves the ability of an individual to say, "I don't want my information used," while preserving the cost effectiveness of gathering and retaining data. Opt-out starts with the premise that a particular database may be used for marketing purposes. It is of note that use of data to reach out to inform consumers of products in fact can make consumers more knowledgeable of an array of a given product in order to make more informed choices. From that point individuals, via opt-out, can ask to be removed from such lists, preserving their privacy. All they need to do is ask. From a cost basis, the opt-out database need not be built from scratch, as is the case with opt-in. The number of responses from consumers, whether opt-out or opt-in, will be relatively small when

compared with the overall size of a database. In the case of opt-out, those who wish to do so may, but the cost of the resulting database remains relatively low and the size of that database which may be used will be relatively large and useful. In the case of opt-in, the relatively small number of responses will make the database small and costly, since the database will be built from the ground up.

Related to opt-out is the concept that information may be freely shared among affiliates, and that opt-out only applies to those situations where the information is shared with third party non-affiliates. NAII supports these concepts under GLB as being equitable, in that the free information sharing among affiliates would, for example, place any stand-alone financial institution at a disadvantage without an ability to share with non-affiliates. GLB strikes a proper balance by permitting the opt-out in the non-affiliate situation, while protecting the consumer via the requirement of a confidentiality agreement.

On the subject of nonpublic personal information, NAII believes Alternative B which states that if the information is publicly available, it is not nonpublic personal information is the more workable. Alternative A would require entities to set up a costly "tracking system" whereby should the information come in via an application, all that information becomes personal, regardless of its availability in a phone book, for example.

Regarding joint accounts, NAII believes that the primary person on the account should be the one to whom notices are sent and to whom the right to opt-out applies. From the insurance perspective, companies normally have a single "named insured" or primary

person on a policy. From a banking perspective, this occurs in the same manner as is currently practice regarding a joint account: only one party's social security number is taken for tax reporting. In both cases, normally only one person gets the ongoing information, whether a copy of an insurance policy or renewal, or a bank statement. To require otherwise would impose impossible burdens. First of all, should all account holders opt-out, a majority? It is also virtually impossible to split out the personal information on one account holder from another. From an insurance perspective, it could require notices to spouses and children on an auto policy to possibly anyone living in a household on a homeowner's policy.

NAII strongly urges the federal regulators to permit third party contractors to use information received from financial institutions to improve credit scoring models or analyze marketing trends so long as the information is maintained in a manner that does not allow for identification of a particular consumer. Information that does not identify particular consumers does not jeopardize individual privacy and should be generally available for research. Inhibiting research based on non-identifiable information would inadvertently thwart important public policy objectives in which use of non-identifiable data would play a critical role.

Six month's time after adoption of the rules is simply not realistic for financial institutions to comply with the rule. The privacy rules stemming from the GLB Act will, to the financial services industry, be rules of first impression. They will require significant systems changes and testing as well as personnel training. Many institutions

will also have to grapple with how to comply with regulations from the federal reserve, OCC, OTS, FTC, state insurance departments, FCRA, and HIPAA before they can even begin the practical aspects of implementing the GLB Act. In addition, many states will have to enact enabling insurance legislation before insurance regulations can even be drafted. NAII urges the federal regulators to extend the period of time so that much of the GLB Act privacy procedures would be capable of being implemented on a phase-in basis, whether by regulation or as a matter of course.

Specific Comments

1. Under the heading: Purpose and Scope, the FTC requested comment whether an entity engaged in, for example, real estate settlement servicing is a “financial institution” only if it also extends credit or services loans, or whether real estate settlement servicing alone constitutes a financial activity that results in an entity that engages in that activity being classified as a “financial institution." NAII urges the federal regulators to avoid creating an unlevel playing field between entities that perform a particular service and financial institutions performing the same. The former would be free of privacy regulation while the latter would not. NAII believes that, however brought about, the result should be that entities engaged in a given function should be similarly regulated.

2. NAII supports the use of examples in the Rule as being useful to illustrate compliance with the Rule. Consistent with the principle of uniformity among federal regulators, however, NAII urges that the examples differ only to the extent necessary to

accommodate the differences between different types of financial institutions and should not reflect any policy differences.

3. The FTC rule requested comment as to applicability to debt collectors. NAII does not comment specifically on this point, but the issue raised the concern of differing standards relating to the same activity. Should consumer A whose bank attempts to collect a debt be subject to differing privacy protections than consumer B whose debt is being independently collected? The functions are the same.

4. The term "significantly engaged" should not be defined, because the nature of financial activities varies greatly among financial institutions, but the nature of the activities may also change almost daily. NAII does recommend the use of examples in the rule, consistent among federal regulators to illustrate what is contemplated by the term.

5. NAII believes that consideration of an individual who operates a sole proprietorship should be considered a financial institution, but only in the context of that sole proprietorship and only to the extent that those functions are similarly subject to GLB for other entities.

6. The issue of including nontraditional financial institutions in the scope of any Rule should be consistent with the overall intent of the GLB Act and should be consistent

over a given function so that the situation does not exist where entity A is subject to the privacy rule while entity B, engaged in the same activity, is not.

7. Service providers for financial institutions should not be considered separate entities under the Rule for purposes of the notice requirement. The customer or consumer is protected by the requirements imposed upon on the financial institution itself. This is the only logical construction since a transaction could involve a number of service providers and the customer or the resulting multiple notices could confuse the consumer.

8. 313.3(j)(3)(iii) should, as the FTC Rule does, have the exception for secondary market sales, securitizations, or similar transactions. It appears that the Rule goes beyond the scope of the GLB Act which in Section 502 (e) states the exception as applying to "a proposed or actual securitization, secondary market sale…" There is no reference in GLB to those entities being "…chartered by Congress…" The reference should be stricken from the rule. NAII generally agrees that information disclosed under the permissible disclosures of 313.10 and 313.11 should not be transferred to others except in the same manner as the financial institution could do so in the original instance.

9. Entities that receive consumers' nonpublic personal information from institutions **chartered by Congress** should be subject to the same limitations on reuse under the rule. As with comment #8 however, the phrase highlighted in bold does not seem to

appear in the GLB Act and should be stricken from the rule.

10. The requirement to execute a confidentiality agreement with non-affiliated third parties should be limited to joint marketing agreements and non-affiliated third parties that perform services on behalf of the financial institution as it is under the GLB Act. The GLB Act does not require confidentiality agreements under the exception circumstances. Executing a confidentiality agreement with some third party non-affilitates such as, federal, local or state authorities, could be difficult if not, impossible.

11. As indicated in the opening comments, the standard for defining nonpublic personal information should be "available from" (Alternative B) rather than "obtained from" for the reasons stated above.

12. A variation to current alternatives A and B should not be drafted to require a financial institution to establish procedures to verify that information is, in fact, available from public sources before the financial institution may disclose it as “publicly available information”. Under the GLB Act, financial institutions are prohibited from disclosing non-public information. To comply, companies will ensure that the information was originally obtained from a public source or the information was “publicly available” at the time that it was obtained. Therefore, it is not necessary to require that such procedures be established.

If such a variation is drafted, it should be limited to requiring reasonable procedures for initially determining whether the information was obtained from a public source or publicly available. Public information should be able to be disclosed without independent verification prior to each disclosure. Otherwise, no disclosures of information can ever be made without employing the resources to independently verify whether the information is currently "publicly available". This would be extremely burdensome on financial institutions to double-check every data element that was publicly available at the time that the information was obtained. There is no reasonable expectation of privacy in information that is, or has been, public information.

13. NAII believes that the definition of " personally identifiable financial information" is too broad. We recommend that the agencies adopt a standard that limits the definition to information that actually describes a consumer's financial condition such as account balances, payment history, overdraft history, income, and assets and liabilities. We do not believe that the examples in the proposed Rule constitute financial information, and we urge the agencies not to characterize all the information on an application or the mere fact that a customer relationship exists as "personally identifiable financial information". In addition, such an expansive definition could result in the same piece of information being subject to a number of different privacy standards such as the HHS's HIPAA regulations and the Fair Credit Reporting Act (FCRA).

The Fair Credit Reporting Act (FCRA) provides an excellent format for defining financial information. The FCRA regulates the use and disclosure of consumer reports which includes information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility" for credit, personal lines insurance, employment, etc. The FCRA also recognizes transaction information. We believe that consumer report and transaction information cover the type of financial information that should be protected. It is advantageous to use definitions from the FCRA because both financial institutions and agencies have experience in applying those definitions. Additionally, many financial institutions currently provide an opt-out under the FCRA and using the same definitions in these regulations would help to avoid customer confusion as to the scope of the two opt-outs.

14. One request for comment related to whether further definition of "personally identifiable" would be helpful. NAII urges the federal regulators to do so, but in such a way as to create consistency with the FCRA. NAII further urges the federal regulators to closely scrutinize other federal privacy laws to seek uniformity in any such definition to the greatest extent possible.

15. NAII believes that the appropriate alternative for defining publicly available information is Alternative B. Alternative A is unworkable in that it requires costly

tracking of the data as it comes into the entity and each time the information is updated or verified. Under Alternative A, the same piece of information could be characterized differently depending upon the source of the information. Also, Alternative A has a very restrictive list of sources from which "publicly available information" exists. Alternative B is more flexible and realistic.

16. NAII supports a statement that information available over the Internet is publicly available if no password is required to access the information.

17. Regarding joint or multiple party accounts, please refer to the comment in the general comment section. NAII urges the regulators to adopt a "primary party" concept in relation to such accounts. The primary person would be the one to receive all notices (as currently is the case for banking and insurance transactions) and to exercise all rights and/or options. This standard avoids confusion and administrative burden for consumers and financial institutions.

18. NAII strongly agrees that the standard for providing notice should be one of a reasonable time. Some cited examples include secondary markets and where there is no choice about the purchase. From an insurance perspective, the consumer may have an immediate need for automobile coverage while at the lender or dealership, or could even be phoning in for coverage to obtain a license or registration. Coverage needs to be provided immediately, but written notice may be impossible. Thus, a general rule that the notice should be at a reasonable time after the transaction is

appropriate.

Additionally, NAII believes that the notice of privacy practices and opt-out be permitted, under reasonable circumstances, via telephone. Telephonic transaction of business occurs in all segments of the market, insurance and otherwise. The rule could address this by requiring entities doing business telephonically to have in place procedures to address these issues.

19. Just as the wishes of a consumer to opt-out of use of information is appropriate under certain circumstances, unique consumer requests such as whether to not receive information or to have it sent to a different location, should be capable of being honored without causing a violation of the rule.

20. NAII recommends a flexible rule geared to accept consumer requests for special handling of notices. Perhaps "reasonable under the circumstances of the particular transaction" would suffice.

21. It is unrealistic to limit transactions to those which lend themselves to notice by mail to the consumer. NAII recommends that the rule be structured to permit non-mail notification where appropriate to the transaction or at least by mail as soon as reasonable.

22. We believe that the applicable standard for determining whether an account is dormant, and thus not subject to the annual privacy policy notice requirement, should be the financial institution's own internal policies on terminated accounts. As a general rule, a financial institution's policy on terminated accounts will be consistent with applicable law. To the extent possible, the regulations should allow institutions the flexibility to provide privacy notices only when such notices will be meaningful and relevant to the consumers that receive them.

23. NAII believes that a flat 12-month standard of no communication with the customer is inappropriate for the reasons stated in #22 above. The rule as proposed could make even a marketing contact to an account which by all normal business standards is dormant, effectively active for the purposes of the 12-month requirement.

24. NAII agrees that under examples in the FTC notice, if the customer and the financial institution orally agree to enter into a contract for a financial product or service over the telephone, then the institution may provide the consumer with the option of receiving the initial notice after providing the product or service. NAII also urges the regulators to permit a reasonable degree of flexibility in the exact timing of the notice taking into account different product distribution methods so that critical business transactions are not delayed.

25. NAII believes the intent and purpose of the notices should be to inform the consumer that personal information might be used. Any requirement listing specific entities to

whom information may be disclosed, rather than entities in general will likely become outdated and incorrect, requiring constant review, correction and new mailings by the institution. All of these are costly and provide little if any new, useful information to the consumer. It is entirely adequate that the notice indicate that the institution may disclose information to entities as permitted by law or, at most, indicate general categories of entities to whom information may be disclosed.

26. The opt-out option for joint accounts should be handled in the same manner as notice for joint accounts: one individual should be designated as the primary party. This is consistent with current insurance and banking practices. Insurers use the terms "named insured" or "policyowner" or other terms to indicate who gets all notices, bills, etc. Likewise, banks on joint accounts assign the account to one person's social security number and send statements to the one name. There should not be consideration of one party or another opting out. Only the primary person should be allowed to do so.

27. NAII believes 30 days is a reasonable time for opt-out when the notice is sent by mail. Any longer time would create an unreasonable burden upon the institution in not knowing what the choice was. Given that opt-out remains an option at any time, 30 days is sufficient. It would be helpful for the rule to contain an example relating to electronic transactions. However, NAII urges the regulators to permit the greatest possible flexibility in methodology permissible for electronic opt-out.

28. Opt-outs should not be required via any means the institution uses to communicate with consumers, as this would place an unreasonable burden on the institution. For example, some institutions have websites that are merely informational, yet the website is a means of communicating with consumers. Must that institution create an interactive website to accept opt-outs? Also, implementation of this standard would require the institution to funnel **any** opt-out, however received, to a central location so that opt-outs can be properly registered. In fact, such a standard could have a reverse effect in creating lost opt-out requests. Clearly, an institution's opt-out should be reasonable in relation to the transaction, but the institution should have the ability to determine the method by which opt-out notice is sent so that the institution can best implement the opt-out. Similarly, if the institution wishes to have more than one method by which to opt-out, that should also be permitted. If the customer relationship is established over the Internet, then that appears reasonable under those circumstances.

29. A reasonable time to provide an opt-out notice provides the best standard in order to address the diverse transactions occurring in the financial service world. Setting a single time lends itself to being too long in some cases and too short in others. As with the initial privacy notice, if the transaction is such that the parties orally agree to enter into a customer relationship, there should be a reasonable time for the institution to provide an opt-out notice.

30. As with opt-out notices, the reasonable time standard for implementation of the opt-out is appropriate. The standard should be based upon the institution's receipt of the opt-out request.

31. The burden of the requirement of opt-out notices is expected to be considerable simply by virtue of the sheer volume of individuals who are to receive the notice. It is naïve to merely include sending out the opt-out notice as part of the burden, as there is the need for establishing the underlying operational aspects of the opt-out, from generating the notice within the appropriate time to removing those who opt-out to changing those from opted-out to opted-in and vice versa. Insurers are expected to widely vary as to the methods used to deliver the opt-out notice. Delivery methods will likely include mail, electronic transmission, personal delivery and other methods. It is impossible to judge the number of opt-out notices which are expected by the industry to be delivered (though the number is likely to exceedingly large) as it is impossible to judge how many opt-out elections will be made to require processing.

32. We believe that the requirements upon a financial institution to “fully disclose” the providing of information to a service provider should be consistent with the requirements for informing consumers about information disclosures to nonaffiliated third parties pursuant to the exception in Section 502(e). To do otherwise would be confusing to consumers since they are not given the opportunity to opt-out of such sharing.

33. NAII strongly urges the federal regulators to permit third party contractors to use information received to improve credit scoring models or analyze marketing trends so long as the information is maintained in a manner that does not allow for identification of a particular consumer. Information which does not identify particular consumers should be generally available for research. Under these circumstances, the protection of the individual's information via opt-out is not relevant.

34. NAII feels that the Rule should not impose additional requirements relating to service providers and joint marketing agreements other than those stated in 313.9. NAII points out that many smaller institutions rely heavily on third party service providers or joint marketing arrangements in their operations. Additional burdens could limit competition via increased costs to the smaller entities by requiring the operations to be taken on in-house or forcing acquisitions; or by precluding the smaller entities from operating in certain areas altogether.

35. It is wholly inappropriate to require specific safeguards to be added to the consent to minimize the potential for consumer confusion. The theme behind the rules should be that there be a reasonable balance between protecting privacy of information and preserving the utility of such information. Creating specific requirements believed to safeguard consumer protection will immediately impose on institutions specific burdens which will not be consistent with reasonable provision for notice to consumer. NAII maintains that the establishment of any specific standards is

counterproductive, and forcing businesses to conform to those standards is clearly contrary to the streamlining of business envisioned under GLB.

36. There is no need for the rule to require a financial institution to develop policies and procedures to ensure that the third party complies with the limits on redisclosure of the personal information. It will likely be in the best interest of the financial institution to do so, and also, may be in the best interest of the third party to establish procedures. There is no need to draft language in the rule requiring the entities to do so. Such language would be incapable of addressing the variety of situations which may arise.

37. Comment was requested on whether the proposed rule 313.12 would restrict a third party nonaffiliate from using information obtained in accordance with the rule's exceptions for purposes beyond those exceptions if the information is not in personally identifiable form. NAII believes information, devoid of personally identifiable information, should be permitted to be used for research and other informational purposes. The need for individual privacy protection is removed when the part of the information identifying the individual is no longer there. Also see comments to #33 above.

38. NAII believes the term "lawful" in the context of Section 502 (c) means that the disclosure, if made by the original financial institution, would be permissible under

GLB.

39. It appears that under Section 502 (c), the third party nonaffiliate may only disclose information received pursuant to the exception in 313.9 of the rule provided the originating financial institution may make such a disclosure. The appropriate test is that relating to the original financial institution.

40. A subsequent disclosure by a third party appears to be lawful where the financial institution is not a party to the subsequent disclosure, but only in those situations where the facts of the disclosure by the third party constitute a circumstance under which the original financial institution could disclose the information.

41. NAII does not have a position on instances where disclosure of account number information for marketing purposes would be appropriate.

42. There may be instances where third parties act as general service providers of information which may contain account numbers. Hence a flat prohibition of any account number, access code, etc., would be inappropriate. Often, a marketing piece may be enclosed in the same envelope as the statement. Or the marketing wording about a product may be typed on the monthly account statement. NAII suggests that in situations where, in the normal course of business, a service provider has access to account information, that marketing materials be permitted where the marketing materials are in addition to the account information and the marketing materials are

not linked to the account information other than being in the same medium. This would also allow marketing via the Internet where account information is accessed via the Internet. NAII suggests a reasonableness standard for such circumstances.

We urge the regulators to clarify that account numbers that do not include internal reference numbers that a financial institution may generate to identify individual customers but that are not sufficient to gain access to funds or commit additional financial obligations. For example, membership companies frequently assign a "member number" to our customers to confirm eligibility for certain products and to provide a unique identifier that all affiliates and approved third-party vendors can recognize; however, the member number alone is not adequate to allow an individual to debit or credit accounts, credit cards, insurance policies, or investment accounts. Use of the member number simply allows the financial institution to speed up service to its customers.

43. We believe that the regulators should provide a clarification that the limitation on the provision of account numbers is only to restrict disclosure of account numbers for marketing of the "nonaffiliated third parties'" products of services. The exceptions in Section 502(e) of the statute clearly express the recognition that financial institutions use third parties to market and process the financial institution's own product and services and that the sharing of account numbers for those purposes may be a necessary part of such processes.

44. NAII questions the need for an institution to disclose account numbers in encrypted format without providing a marketer the key to decrypt the number. However, such a circumstance may, from a practical standpoint, be more cost effective than sending individual information first encrypted, then sending the key. One example would be where the institution provides the entire database with encrypted numbers, only to be accessed with a key for individual accounts. In any event, NAII believes such disclosure should be permissible if reasonable under the circumstances. NAII also believes that any requirements in this area should be technologically neutral.

45. Six months following adoption of a final rule is not sufficient for financial institutions to comply with the rule. The privacy rules stemming from GLB chart a new territory of regulation and require sweeping changes not only as to systems, but also as to the mindset behind doing business in the new financial services world. NAII urges the regulators to extend the period of time so that much of GLB privacy procedures would be capable of being implemented on a phase in basis, whether by regulation or as a matter of course. An additional benefit is that if institutions send out initial notices at differing times, as well as opt-out materials, the consumer will not be inundated with materials on privacy from each financial institution the consumer deals with on, say, November 12, 2000. NAII recommends a two-year phase in period, with a moratorium on any enforcement and penalties. Just as significant, the same institutions would (within one company structure) have to comply with regulations from the Federal Reserve, OCC, OTS, FTC, state insurance departments,

FCRA, HIPAA.

46. The 30 days to deliver notices after effective date of the Rule still raises the fact that consumers will be inundated with notices from a myriad of institutions in a very short time. NAII submits that much of the meaning behind a privacy notice is thwarted under such a scenario. Please see comments to #45 above.

47. NAII believes that the rule can impose burdens upon small entities, especially those not part of an affiliated financial services structure. For example, while a bank and its affiliated insurers and other entities can share some information which consumers cannot opt out of sharing, the smaller entity must maintain a system under which opt out is processed in situations of dealing with nonaffiliates. Also, as the rule places burdens on all entities, economies of scale make the burden effectively greater on smaller entities.

48. NAII believes that other federal privacy laws, mentioned earlier, are in some instances duplicative and in others conflict with the proposed rule.

NAII appreciates the opportunity to comment to the proposed rules. Should there be any questions relating to these comments, please contact Michael Koziol, Senior Director and Counsel, NAII, 2600 S. River Road, Des Plaines, Illinois 60018. Phone: 847 297 7800. Fax: 847 297 5064. Email: mkoziol@naii.org.

Comments or questions may also be sent to: Julie L. Gackenbach, Director of Government Relations, NAII, 444 N. Capitol Street NW, Suite 801, Washington, D.C. 20001. Phone: 202 639 0473. Fax: 202 639 0494. Email: jgackenb@naii.org.